



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,147	02/27/2002	Jeff A. Shaw	884.630US1	1264

7590

09/07/2005

SHARMINI N. GREEN
C/O BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER

ELMORE, JOHN E

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/085,147

Applicant(s)

SHAW, JEFF A.

Examiner

John Elmore

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 February 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 10-16, 19-22, 24-26 and 28-42 is/are rejected.
- 7) ☒ Claim(s) 4-9, 17, 18, 23 and 27 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 February 2002 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-42 have been examined.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 1-3, 10-14, 16, 18, 20-23 and 35-38 are rejected under 35**

U.S.C. 102(e) as being anticipated by Freund et al. (US 2003/0055962), hereafter Freund.

Regarding claim 1, Freund discloses a method for on-connect security scan and delivery, comprising:

interfacing with a remote access infrastructure to detain a client in a virtual lobby when the client attempts to connect to a network (client detained when attempting to access network/Internet; col. 7, para. 0070 and 0071);

scanning the client to determine if the client complies with security requirements (client is scanned to ensure compliance with security policies; para. 0071 and 0072);

and

permitting connection to the network only if the client complies with the security requirements (para. 0072).

Regarding claim 2, Freund teaches all the limitations of claim 1, and further teaches interfacing with at least one provider of at least one security mechanism to bring the client into compliance with the security requirements, if the client is not in compliance (interfacing with sandbox server 360 to bring client into compliance; para. 0071).

Regarding claim 3, Freund teaches all the limitations of claim 1, and further teaches retrieving client information from a repository (client information stored in router compliance table and is retrieved upon client access attempt; para. 0144 and 0145).

Regarding claims 10-12, this is a system version of the claimed method above (claims 1-2). Therefore, for reasons applied above, such claims also are anticipated.

Regarding claim 13, Freund teaches all the limitations of claim 12, and further teaches that remote access infrastructure processes at least dialup and virtual private network (VPN) connections (para. 0060 and 0068).

Regarding claims 14 and 16, this is another method version of the claimed method above (claims 1-2) with the additional limitation of controlling configuration of a plurality of security mechanisms for a client based on security requirements for a network (compliance monitoring controls a plurality of security mechanisms, including MailSafe, ZAP, and other antivirus programs; para. 0071, 0106, 0112 and 0117). Therefore, for reasons applied above, such claims also are anticipated.

Art Unit: 2134

Regarding claim 18, Freund teaches all the limitations of claim 14, and further teaches presenting a security warning to the client (para. 0115 and 0116).

Regarding claim 20, this is a system version of the claimed method above (claim 1). Therefore, for reasons applied above, such a claim also is anticipated.

Regarding claim 21, Freund teaches all the limitations of claim 20, and further teaches a repository component in communication with the computing system to store the security requirements (client information stored in router compliance table and is retrieved upon client access attempt; para. 0144 and 0145).

Regarding claim 22, Freund teaches all the limitations of claim 21, and further teaches that the repository component is a database management system (it is inherent that a router or other device containing a data table also contains a data management system where data is added and removed from the table).

Regarding claim 23, Freund teaches all the limitations of claim 21, and further teaches that the repository component operates to manage the security requirements and associated delivery instructions for available security mechanisms (device 310 operates to manage security requirements indicated by compliance table 312 and to manage delivery instructions by redirecting a non-compliant client to the sandbox server 310 at a particular port, which indicates to the server what instructions to provide; para. 0071, 0095, 0098, 0106 and 0117).

Regarding claim 35, Freund teaches a method of doing business comprising:

providing a software product to an enterprise configured to scan clients attempting to connect to a network and to provide delivery of security mechanisms to comply with security requirements (para. 0071);

updating security requirements in the software product (para. 0106 and 0112);
and

integrating delivery of new security mechanisms into the software product when the security requirements are updated (updates in security requirements will prompt updates in client software; para. 0071).

Regarding claim 36, Freund teaches all the limitations of claim 35, and further teaches that providing delivery of security mechanisms comprises providing webpages for downloading (para. 0071 and 0117).

Regarding claim 37, Freund teaches all the limitations of claim 35, and further teaches that the delivery of security mechanisms is semi-automatically integrated into the software product (para. 0071).

Regarding claim 38, Freund teaches all the limitations of claim 35, and further teaches eliminating a security mechanism from the software product when it is no longer needed to comply with the security requirements (para. 0106 and 0112).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 15, 24 and 39-42 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Freund.

Regarding claim 15, Freund teaches all the limitations of claim 14, and further teaches delivering third-party security mechanisms to the client through the delivery assistant (sandbox server 310 facilitates delivery of third-party security mechanisms, including the downloading of security software to the client; para. 0071). But Freund does not explain certifying third-party security mechanisms that meet the security requirements.

However, it is well known in the art that certification provides a simple and efficient means of ensuring that a third-party security mechanism meets security requirements. One of ordinary skill in the art would recognize where a delivery assistant provides security software to a client, the delivery assistant would need to ensure that the security software was authentic and in accordance with security requirements. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Freund to provide for certifying third-party security mechanisms that meet the security requirements for the motivation of providing a simple and efficient means of ensuring that a third-party security mechanism to be installed meets security requirements.

Regarding claim 24, this is a system version of the claimed method above (claim 15). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 39, Freund teaches all the limitations of claim 35, but Freund does not explicitly explain contracting with a vendor to provide delivery of at least one security mechanism.

However, Freund teaches the delivery of at least one security mechanism by downloading security software (para. 0071). One of ordinary skill in the art would recognize that where third-party security software is downloaded, a contract with the vendor of that software is generally required. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Freund to provide for contracting with a vendor to provide delivery of at least one security mechanism for the motivation of legally utilizing third-party software.

Regarding claim 40, Freund teaches all the limitations of claim 35, but Freund does not explicitly explain tracking revenue generated from deliveries to the client over time and delivering at least a percentage of the revenue to the enterprise.

However, the Examiner takes official notice that where an enterprise is a for-profit business and where revenue is generated for the enterprise by the purchase of security software from a vendor and the subsequent sale and distribution of that software to a client, the enterprise would retain a percentage of the revenues generated from the client as profit and that such revenues would need to be tracked in order to be properly determined and retained. , it would be obvious to one of ordinary skill in the art

at the time the invention was made to modify the method of Freund to provide for tracking revenue generated from deliveries to the client over time and delivering at least a percentage of the revenue to the enterprise for the motivation of properly determining and retaining the profit from the resale of software to the client.

Claim 41 is rejected on the same basis as claim 40.

Regarding claim 42, Freund teaches all the limitations of claim 39, and further teaches that at least one security mechanism is an anti-virus software product (among the security software products checked for compliance are anti-virus products; para. 0112 and 0117). Therefore, for reasons applied above, such a claim also would have been obvious.

5. **Claims 25, 26 and 28-34 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Freund in view of Strebe et al. ("Firewalls: 24seven," Sybex, first edition, 2000), hereafter Strebe.

Regarding claim 25, this is an article-of-manufacture version of the claimed method above (claims 1-2) with the additional limitation that the virtual lobby resides between an inner firewall and an outer firewall. But Freund does not explain that the virtual lobby resides between an inner firewall and an outer firewall.

However, Strebe teaches the use of an inner firewall and an outer firewall to create a "demilitarized zone" around a public server for the purpose of enhancing security via two levels of security between a network and devices external to it that may pose a threat (pages 25-26). One of ordinary skill in the art would recognize that the

device 310 acts as a public server in controlling connectivity between networks, particularly in regulating the access of a client to a network.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Freund to provide that the virtual lobby resides between an inner firewall and an outer firewall. One would be motivated to do so in order to enhance security.

Regarding claim 26, the modified device of Freund and Strebe is relied upon as applied to claim 25, and Freund and Strebe further teach providing warnings for select security requirements and permitting the client to connect to the network (para. 0072, 0115 and 0116).

But Freund does not explicitly explain enforcing rules for overriding the select security requirements, wherein the rules for overriding are adaptably defined under the circumstances.

However, Freund teaches that the system administrator has "the option to establish and configure various security policies to be observed and enforced by the system "(para. 0106). The Examiner takes official notice that one of ordinary skill in the art would recognize that since the policy rules exist at the discretion of the administrator, those policies may be defined that override certain select security requirements otherwise in operation. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Freund and Strebe to provide for overriding the select security requirements, wherein the rules for overriding are adaptably defined under the circumstances. One would be motivated to do so in

order to provide the administrator with the ability to adapt the security policies to conform with the changing needs of the system, particularly where those changing needs may conflict with already established security requirements.

Regarding claims 28-30, the modified device of Freund and Strebe is relied upon as applied to claim 25, and Freund and Strebe do not explain teach providing a presentation notifying the client of scanning, of implementation resources information, or of compliance status.

However, it is widely known in the art to inform a client where examination and authorization operations are being performed, particularly where the client where the client is otherwise uninformed of the operation and the operation may cause a delay in completing the client's requested services. And Freund and Strebe teach notifying the client of the results of scanning where a security violation is discovered (Freund: para. 0115 and 0116) and for any other purpose as defined by the administrator (Freund: user prompt; para. 0131). One of ordinary skill in the art would recognize that notification of scanning, of implementation resources information, and compliance status represents commonplace information indicating what operation is being performed with what resources and the status of that operation.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Freund and Strebe to provide a presentation notifying the client of scanning, of implementation resources information, or of compliance status for the motivation of informing the client of the scope and status of

an operation, particularly where that operation may interfere with and potentially cause a delay of requested services.

Regarding claims 31, this is a system version of the claimed article-of manufacture claimed above (claim 25). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claims 32, the modified device of Freund and Strebe is relied upon as applied to claim 31, and this claim is further rejected for the reasons as applied to claims 2 and 3.

Regarding claim 33, the modified device of Freund and Strebe is relied upon as applied to claim 32, and Freund and Strebe further teach that the repository component also holds security policy information (para. 0084, 0085 and 0106). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 34, the modified device of Freund and Strebe is relied upon as applied to claim 32, and Freund and Strebe further teach that the repository component comprises a policy management system (it is inherent that where policies are stored in a device, being added and removed by an administrator, the mechanism for modifying the policies constitutes a policy management system; para. 0084, 0085 and 0106). Therefore, for reasons applied above, such a claim also would have been obvious.

Allowable Subject Matter

6. **Claims 4-9, 17, 18, 23 and 27 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 4, the closest prior art, Freund, does not explain performing a security risk assessment for the network and creating the security requirements to address risks identified in the security risk assessment.

Freund teaches only that the client network is checked for compliance with security policies, notably the proper operation of any security assessment applications running on the client (para. 0071 and 0121). Freund makes no suggestion that the compliance monitor protocol performs a security risk assessment for the network other than checking for the proper operation of applications that perform such security risk assessments. And even if the compliance protocol itself is considered a form of security risk assessment, the security requirements associated with the compliance assessment are created prior to the assessment by the system administrator and not as a result of the assessment (para. 0106).

Gaul (US 2001/0034847) teaches a method for performing a security risk assessment of a network from a remote risk assessment tool (NVST application scans targeted network from a remote server; para. 0031-0033) for the purpose of permitting a security risk assessment provider to determine the vulnerability of a network from a

remote location (para. 0014 and 0015). However, as there is no suggestion in Freund that the compliance monitoring protocol or the sandbox server perform or call a third party provider to perform a security risk assessment, particularly in response to a network connection attempt by the client, it would not seem obvious to modify the method of Freund with the teaching of Gaul due to a lack of motivation.

Claims 5-9 are allowable by virtue of their dependence on claim 4.

Regarding claim 17, the closest prior art, Freund, does not explain providing an optional delivery to the client. Freund teaches that the security compliance monitor protocol requires the client to adhere to all security requirements in order to gain network access. As Freund provides no motivation for optional delivery, and such a mechanism in this context is not widely known in the art, it would not seem obvious to modify the method of Freund to provide for optional delivery to the client.

Regarding claims 18 and 27, the closest prior art, Freund, does not explain scheduling a future delivery to the client. Freund teaches that the security compliance monitor protocol and the sandbox server facilitates the adherence of the client to all security requirements prior to gaining network access, including the downloading of any security software, but Freund makes no reference to a means for scheduling the downloading of software or other delivery to the client, much less for completion at a future time period. As Freund provides no motivation for scheduling a future delivery, and such a mechanism in this context is not widely known in the art, it would not seem obvious to modify the method of Freund to provide for scheduling a future delivery to the client.

Regarding claim 23, the closest prior art, Freund, does not explain that the repository component operates to manage the security requirements and associated delivery instructions for available security mechanisms.

Freund teaches that the repository component (compliance table 312), which stores the client information, resides on a device on the client's premises (para. 0069) and that the sandbox server, which provides the delivery instructions, resides at a remote location to the client and stores no client information, instead relying on port information to determine non-compliance and prescribe instructions (para. 071 and 0095).

Conclusion

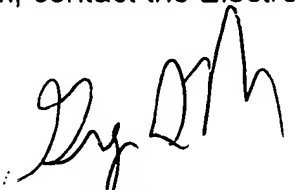
Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

John Elmore



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100